Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1830 07/29/16

~ VPN Use in UAE Illegal! ~ Ransomware Victim Help? ~ Atari’s 3DO Console!

-* KeySniffer Steals Keystrokes *-
-* Trying To Kill Net Neutrality Again! *-
-* Microsoft Is Updating Windows 10 Again! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Firstly, let me apologize for the excessive delay with this issue. I knew that it might be a littler late because I was scrambling for enough articles to make the issue, but then I realized what day it was. You see, I put A-ONE together using a number of "tools" on a PC. Lack of room years ago put me in the position of having to mothball my Atari machines; I haven’t found space to put them back into service yet. Getting back to the date - it was the last day that Microsoft was allowing customers to upgrade to Windows 10 for free. We bought PC less than a year ago, but decided to wait before installing Windows 10. I had heard enough horror stories that I wanted to wait. Well, we decided to upgrade for free rather than pay later.

Getting Win 10 took a lot longer than I anticipated. My system installed all of the outstanding upgrades for Win 8.1 - either something that it had to do, or user error on my part. I also backed our systems up ahead of time, just in case! Next came the Win 10 download, which took forever! And finally, installing the upgrade! I started just after lunch when I got home from work; the upgrade finished a little after 9:00 p.m. Let’s just say that I was exhausted, and there was no way I was going to be able to put the issue together for our usual Friday release deadline!

Well, I primarily use NotePad and WordPad to edit and put the weekly issue together. The Win 10 versions of those programs are a little different from their predecessors. And WordPad is very different. None of my A-ONE templates stayed formatted correctly under either program, so I’m still playing around making that happen. This week’s issue was done purely in NotePad - not a great replacement for a pseudo word processor! I have no idea what the final appearance will be on your end, yet! But, the show must go on, some way, some how - so here we are, a few days late! You have no idea how much I miss being able to use the Flash 2 TA buffer on my Atari Falcon!

I was going to comment on the presidential conventions, but I’ll forego those comments due to lack of time. Thankfully, they’re over!

In the meantime, let me get this issue out the door, and maybe I’ll have a few extra minutes to take a walk around the block and play some Pokemon Go! Yes, I have become mildly addicted to this "new" phenomenon!

Until next time...

=~=~=~=

Firebee News Update: Delivery Delay of the New Series - The Whole Truth

The new FireBee series should already be delivered by now. Today we will ruthlessly uncover why this isn’t the case yet. Read here exclusively what ACP has to fight with. Some already had a hunch; others were informed in personal mails about it. Now, the whole world will come to know. The new series of FireBee computers has a delivery delay.

It all began with the fact that the orders for the new series were processed in the new year - after the holidays. Unfortunately, the Swiss manufacturer could not meet the production period of 12 weeks that was agreed upon in 2015. Therefore, the new agreement was that the computers would arrive at MCS around the end of May 2016. But then there was another delay at the manufacturer, and the end of June was communicated to MSC as the new delivery date (including an apology for the delay). So far, everything was still just about OK, especially since we had decided to also produce the LED-/speaker-clips, which would have delayed the production by a few more weeks anyway.

In the meantime, a new problem also arose in Vienna (sounds almost like a global enterprise...). The producer of the cases, with whom it had been a pleasure to work with so far, suddenly wanted to increase the prices of the mini-cases by 24% for the final order. Our hint that this would represent a 100% inflation was countered by a minimal "price reduction" and a brief explanation. The price increase was explained with, among other things, "that all screws would be included now..." At that point, all our trust had vanished, since the cases contain exactly one single screw - the black knurled screw on the lid. And those were always provided by ourselves in the previous series. Since we were not willing to accept an increased price (which we would have had to pass that on to you by a 100%) for inexistent screws, we started looking for a new producer for our cases, as we were convinced that you would prefer waiting for another 4-5 weeks to increased costs.

We now have the new producer, and we also can keep the price of the mini-cases. As soon as we had that, and (thanks to Milan Tirnanic) also a new, perfectly constructed 3D-model of the mini-case, the new computers arrived at Medusa on July 1st. And: none of them work! Most of the boards wouldn’t even start. A few would boot, but then suck so much power that the 45W PSU failed.... so, more a heating device than an Atari clone.

Fredi Aschwanden has spent the last three weeks trying to find the reason, which is proving to be anything but trivial. To this date we don’t know what is wrong with the computers. It could be a short-circuit anywhere in the system. Or some parts were badly soldered to the boards, or the boards themselves might even be defective, or defective parts were used. As of now, the manufacturer has received one of the boards from us, and is removing all the parts and soldering new ones on it. Hopefully this will result in an indication of the source of the problem.

Despite these problems we are really glad to work with a Swiss manufacturer, who is accessible and trustworthy. The bad production will be fixed without additional costs. We’re please not least because aside from the Medusa and the Hades, the first FireBees were also produced there. Had we chosen to let them be produced somewhere in Asia, we would

now have a truly serious problem and could probably write off the money, or file a lawsuit in China (haha).

So we are confident that we will eliminate the problems by the end of August, but we don’t want to make any specific delivery promises here, except that you will receive 100% working FireBees, including two years warranty, for your money. As soon as there is more news, we will inform you here.

=~=~=~=

=~=~=~=

Old-School Sonic Mania Is Coming for Sonic s 25th Anniversary

Sonic the Hedgehog is 25 years old this year, and the blue bur is getting two new games to celebrate even though they won t see release until 2017. In a fitting tribute to a character who s found limited success in modern times, Sonic Mania will take the series back to its roots and give the fans the 2D, sidescrolling Sonic sequel they ve been waiting for.

We re not talking about any broken-physics, Sonic 4 nonsense here, either. Mania is the real deal, with reimagined levels from the Sega Genesis Sonic games (and Sonic CD) as well as new ones and gameplay that matches that of the series 90s glory days. There s also at least one new movement technique and some smoothed out sprite animations, but the game looks decidedly, gloriously old-school in a way only fan projects have managed to capture in the post-Genesis era. Finally, Sega is giving the people what they want.

Mania was announced on Friday alongside Project Sonic 2017 (which is clearly supposed to be the next great modern entry in the franchise, but putting a year next to it just gives me bad memories of the terrible game that s come to be known as Sonic 06) as part of a 25th anniversary celebration live stream that did not instill the kind of confidence that the retro gameplay video did. Sonic 2017 only got a cinematic trailer, so it s hard to say what the actual game will be like, but it once again features modern and classic Sonic side by side like Sonic Generations.

Right now, Mania (which features Sonic, Knuckles, and Tails as playable

characters) is only slated for the PlayStation 4, Xbox One, and PC in spring 2017, with no mention of Nintendo hardware. You can watch additional gameplay footage here for more retro goodness, including some pretty great music. Sonic 2017 is arriving on those same platforms, along with Nintendo s mysterious NX, for the 2017 holiday season.

"The Wii U Has No Games", A Study

Of all the complaints levelled against the Wii U over the years, the most common one is usually there aren t any games . With Nintendo putting out some lifetime release figures overnight, let s see how that claim actually holds up.

Before we begin: in case you need this spelled out, nobody literally means there are no games. Everyone knows there are some games. Some of them are even very good games! But with third parties all but ignoring the system, and Nintendo s attentions split between the Wii U and 3DS, it doesn t take a retail manager to note that big releases (or, well, any releases) for the console have been few and far between.

But that s a gut feeling, and gut feelings can be out. Numbers, on the other hand...

Here are the figures Nintendo released last night, covering almost every single console and handheld the company has ever manufactured (sorry, Virtual Boy, you were left off the list). They tally every single game released on cartridge/disc on these systems in Japan, the US and Other (mainly Europe), and divide the number between those published by Nintendo and those released by OEMs (third parties).

Taking a look at these numbers, the NES saw 72 games released in the United States by Nintendo, with a further 590 games coming from third parties. The SNES breakdown was 52/667, the N64 was 53/244, the GameCube had 48/504 and the Wii a staggering 55/1206.

Two things jump out at you from those numbers. Firstly, the number of first-party releases was fairly consistent. Second, holy shit, look at those Wii figures.

Now to the Wii U. To date Nintendo has released 39 games in the US, while third parties have released just 118. While the system isn t quite done just yet, the few games left in the pipeline (and the NX s imminent reveal) won t move those numbers much.

It s important to note that the Wii U figure doesn t include games (like indie titles) that were only released digitally. And that some of those earlier third-party figures, especially on the Wii, are inflated due to a mountain of shovelware. So the discrepancy between the company s last two consoles isn t quite as immense as it first seems.

In terms of big releases, though, that s still a big drop-off in support from earlier consoles, especially when you look at the Nintendo numbers (which are normally the biggest/best games on a Nintendo system). And while you can argue that the Wii U has had a pretty short life cycle, you can also argue in chicken-and-egg fashion that the lack of games has played a part in that (and also point out that the GameCube s lifespan was just as brief).

Aside from that? Feel free to make even more guesses as to what it all means. You could ponder that the Wii U has been a case of quality over quantity, as despite the overall scarcity it still saw classics like Super Mario 3D World, Super Smash Bros., Super Mario Maker, Mario Kart 8 and Pikmin 3. You could also argue that the lack of big, original games in the Zelda and Metroid series left a gaping hole in the system s catalogue, and that the complete abandonment of major third party titles after the release of the PS4 and Xbox One killed one of the console s original selling points (remember, the Wii U was originally marketed as being a Nintendo console you could also play games like Assassins s Creed III and Deus Ex on).

Me, I think I m going to stick to this: that the Wii U s dry spells would make me forget I even owned one for months at a time. But when the rains did fall, like re-visiting a sunken Hyrule in HD or enjoying Yoshi s Wooly World with my kids (and literally playing with their Amiibo, like adorable, immovable action figures), they were still some very good times.

Overall Console Sales Were Down for June 2016

According to sales number released by the NPD Group, hardware sales declined by 42% over the same period last year.

In its monthly statement, the NPD Group said "Eighth-generation hardware," meaning Xbox One, PS4, and Wii U, were the "primary driver" of the decline, with sales across the 3 down by 43% over June 2015.

Sales of both hardware and software were down, something the NPD Group attributes to a lack of major title launches such as last year’s Batman: Arkham Knight.

Nintendo released a statement saying sales of the 3DS were up 39%, but that increase is month-to-month, rather than year-over-year as is the case with numbers from the NPD Group. Nintendo attributes the increase to the newly discounted 2DS, which can be bought for $80.

Nintendo also revealed lifetime sales of Super Smash Bros. for Wii U have no passed 2 million unit mark in the U.S., with the 3DS version of Smash passing 3 million.

NPD reported sales for PS4 and Xbox One are ahead of their predecessors by 40% when compared to the same period in the PS3/Xbox 360 life cycles.

At the end of May, Sony revealed lifetime sales of the PS4 had reached 40 million units worldwide.

NPD now reports sales of digital copies of games in addition to physical copies. Overwatch was June 2016’s best selling game.

Man Crashes Car Into MapleStory Developer’s Office, Said Its Games ’Ruined’ His Life

A man on Sunday crashed a car into a South Korean game developer’s

office, claiming its games "ruined" his life.

The Chinese man, surnamed Lee, was in South Korea visiting when he decided to drive his older brother’s car into developer Nexon’s offices, reports the Korea Herald.

A PC and mobile game studio, Nexon is known for titles like MapleStory and Atlantica Online. Lee told police he had become addicted to the company’s games and impulsively decided to crash the car into the company’s office, according to the publication. His blood alcohol level was over the limit when tested by local police.

Video game addiction is a real thing with many publicised cases - particularly in South Korea. A two-year-old boy died in 2014 after his father left him unattended for several days to play video games. In 2010, a three-month-old child starved to death while her parents played a game, which ironically involved raising a virtual child, at an internet cafe for days.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

What if Atari Released Their 3DO Console?

It is no secret that when Atari released their Jaguar console that they were going up against the 3DO. In some markets there were other options such as the CD32 (Amiga based) console and other lesser known platforms. This was all prior to the launch of the Playstation (which would kick everyone in the butt) and the Sega Saturn consoles. What if Atari had licensed the 3DO hardware and released a version of it instead of the Jaguar? There is proof that Atari had a 3DO prototype running, there were even games released for it.

Before we get too far into this article it is probably worth mentioning that there were two Atari s for many years. Atari Games was the arcade arm of Atari while Atari Inc was the home platform division. It is the arcade arm that licensed the 3DO hardware but it is unknown if that license was exclusive to arcade machines or if the home division would be able to make use of it too. I am basing this article on the assumption that the home division could use the hardware also.

I am not going to bore you with technical speak, suffice to say that Atari modified the 3DO hardware almost creating a new platform. Atari was floundering quite hard when they released their Jaguar console which did not help their bottom line.

3DO was created from a group of companies coming together to make a console on the revolutionary idea of licensing out the hardware to others to make. It was to be the computer market meets the console market- there are tons of computers over the years that run the same software in varying levels of quality. 3DO was to have a minimum hardware specification and

compatibility requirements- outside of that licensed manufacturers could improve all they wanted. Some were planned with improvements such as the AT&T 3DO which was to come with a modem (none of the other 3DO consoles offered that).

There were two games known at this time for the Atari 3DO- Beavis and Butt-Head and Die Alien Scum. Beavis and Butt-Head appears to have been a 3D brawler similar to Final Fight and Streets of Rage. Die Alien Scum looks to have been shaping up to be a 3D rails style shooter like Total Eclipse or maybe free roam like Star Fighter.

It would have been interesting to see Atari throwing their hat in the ring with 3DO rather than developing the Jaguar console. What do you think? Would saving the R&D costs of the Jag maybe turned Atari s fortunes around just a little longer?

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Broadband Industry Tries Again To Kill Net Neutrality and Title II

Six weeks after federal judges preserved net neutrality rules for the broadband industry, ISPs are seeking a full court review of the decision.

ISPs' attempt to overturn the Federal Communications Commission rules were rejected when a three-judge panel of the US Court of Appeals for the District of Columbia Circuit voted 2-1 in favor of the FCC. Now the broadband industry's trade groups are seeking an "en banc" review in front of all of the DC Circuit court's judges instead of just a three-judge panel. If this fails, ISPs can appeal to the Supreme Court, but the odds against them winning appear to be long.

One en banc petition submitted this morning before the case's deadline came from the National Cable & Telecommunications Association (NCTA) and the American Cable Association (ACA), the two biggest cable lobby groups. En banc petitions were also filed by CTIA The Wireless Association, the mobile broadband industry's primary lobby group; the United States Telecom Association (USTelecom) and CenturyLink (representing DSL and fiber providers); and a small Texas ISP named Alamo Broadband.

"We don t celebrate this petition, but we believe this action is necessary to correct unlawful action by the FCC," the NCTA wrote today. The cable group claims to support net neutrality protections but not the related reclassification of Internet service providers as common carriers. While the FCC passed net neutrality rules using weaker underlying authority in 2010, Verizon successfully sued to overturn them. That proved to be a hollow victory, as it led to the FCC using its stronger Title II common carrier authority to police the broadband industry in its latest set of net neutrality rules.

"As regulators for decades have acknowledged and consistently determined, dynamic Internet networks do not resemble or deserve to be treated like archaic telephone systems," the NCTA wrote.

FCC Chairman Tom Wheeler said today's petitions were expected and predicted that the FCC will win in court again.

It comes as no surprise that the big dogs have challenged the three-judge panel s decision," Wheeler said in a written statement. "We are confident that the full court will agree with the panel s affirmation of the FCC s clear authority to enact its strong Open Internet rules, the reasoned decision-making upon which they are based, and the adequacy of the record from which they were developed.

The NCTA/ACA petition argued that the FCC didn't provide good enough reasons for its net neutrality order, saying that a more detailed justification was needed because the Title II reclassification "rests upon factual findings that contradict those which underlay its prior policy." The DC Circuit panel judges "paid only lip service to these principles," the petition complained.

The NCTA/ACA petition also claims the FCC didn't give the industry adequate notice before imposing Title II regulations on broadband.

The CTIA's arguments touched specifically on mobile broadband, which had enjoyed weaker requirements until the FCC's Title II order put fixed and mobile broadband under the same regulatory scheme. The FCC "unlawfully reclassified mobile broadband" based on a finding that mobile broadband service is "interconnected" with the traditional telephone network, the CTIA said. Mobile broadband's interconnectedness with the phone network was one of the findings made by the FCC in justifying its decision to reclassify cellular Internet access as a common carrier telecommunications service.

The DC Circuit panel decision said it accepted the FCC's view that "VoIP applications now function as an integrated aspect of mobile broadband, rather than as a functionally distinct, separate service. The CTIA disputed this, writing that "Mobile broadband service does not offer the ability to make phone calls just because consumers can use their connection to interact with distinct services offered by different companies that perform the functions needed to bridge the gap between the Internet and telephone lines."

USTelecom and CenturyLink argued that Congress never intended to give the FCC Title II authority over Internet service. "En banc review is necessary to ensure that a largely unaccountable agency does not obtain significant legislative and judicial power that Congress never delegated to it," their petition said.

Last year, CTIA, USTelecom, CenturyLink, and AT&T all claimed the FCC violated the First Amendment with the net neutrality rules. But today, the Alamo Broadband petition was the only one to make a First Amendment argument.

The judges' panel erred when it concluded that the First Amendment does not limit the FCC s authority to regulate Internet service because "the rules strip broadband providers of their First Amendment right to exercise discretion about whether and how to carry Internet traffic over their networks," Alamo claimed. "The Panel s rationale would allow the government to not only order the blocking of Internet content it deems

objectionable, but could also be used to try to strip other media cable operators, broadcasters, and new media conduits of First Amendment protection by declaring them to be common carriers."

Is Russia Behind the DNC Hack To Help Donald Trump? FBI Initiate an Investigation

On [last] Friday, just three days prior to the start of the party's national convention, WikiLeaks released almost 20,000 e-mails with more than 8,000 stolen from the US Democratic National Committee (DNC) following a cyber attack in June.

Two days later, on Sunday, DNC Chairwoman Debbie Wasserman Schultz announced her resignation and now had no major role on the party's convention stage.

Many of the leaked emails indicted that the top DNC officials were actively working against the campaign of Sen. Bernie Sanders and strongly favoring Hillary Clinton over Sanders during the primaries, when they were supposed to be neutral.

The controversy ruined the start of the DNC's national convention in Philadelphia and forced the Wasserman Schultz to resign.

The leak, from January 2015 to May 2016, is believed to be an attempt by the Russian government to influence the presidential election, some U.S. lawmakers and cybersecurity experts say.

The leak features DNC staffers debating on things like dealing with challenging media requests and coordinating the party's message with other powerful interests in Washington.

The emails were leaked from seven DNC officials' accounts. One email shows how DNC staffers attempted to reference Bernie Sanders' faith in an effort to weaken him in the eyes of Southern voters.

Another represents an attorney advising DNC on how to defend Clinton against Sanders campaign's accusation of not living up to a joint fundraising agreement.

From the beginning of the DNC hack, it has been speculated that the breach of the committee's systems exposed in June was the work of Russian intelligence.

Multiple security firms, including CrowdStrike, Mandiant (part of FireEye) and Fidelis, have conducted a forensic analysis of the DNC's systems and found strong evidence linking to "the Russian government's powerful and highly capable intelligence services."

The Clinton Campaign Manager Robby Mook has also argued that Russian intelligence officials are trying to ensure that Republican Donald Trump, who has had an interesting relationship with Vladimir Putin, wins the White House.

"There have been larger forces at work to hurt Hillary Clinton," Mook said. "They [the emails] are being released at this time to create maximum damage to Hillary Clinton to help Donald Trump."

Although Trump has always praised Putin, Clinton has tried to tie Trump to the Russian leader throughout her campaign.

"He praises dictators like Vladimir Putin and picks fights with our friends," Clinton said last month. "Putin will eat your lunch," she once said. Moreover, if Trump were elected President, it would be like "Christmas in the Kremlin," she said.

The Federal Bureau of Investigation is now investigating the DNC breach and is working "to determine the nature and scope of the matter."

"A compromise of this nature is something we take very seriously, and the FBI will continue to investigate and hold accountable those who pose a threat in cyberspace," the FBI said on Monday.

The NSA whistleblower Edward Snowden, currently residing in Russia, has also blasted his host country for its alleged DNC hack.

Despite a staunch supporter of Sen. Bernie Sanders, Snowden condemned the DNC email leaks but pointed NSA's secret data analysis program Xkeyscore that can be used to easily determine the location from which the organization is hacked.

"Even if the attackers try to obfuscate origin, #XKEYSCORE makes following exfiltrated data easy. I did this personally against Chinese ops," Snowden tweeted. Though, he criticized the NSA for not sharing information.

New Portal Offers Decryption Tools For Some Ransomware Victims

Nomoreransom.org, a joint initiative between Europol, the Dutch National Police, Kaspersky Lab and Intel Security, offers help in getting encrypted data back.

Victims of crypto ransomware now have an online portal they can turn to for help in trying to recover encrypted data.

Kaspersky Lab in collaboration with Europol, the Dutch National Police and Intel Security have launched www.nomoreransom.org a site that currently provides decryption tools for four ransomware families and will soon feature tools for several more.

The site provides users will general information on ransomware, how such malware works and how to mitigate exposure to the threat. It also provides an option where victims can upload two encrypted files to the site to help identify the ransomware on their systems and to see if any of the available tools can help decrypt the data.

Ryan Naraine, director of the global research and analysis team at Kaspersky Lab US, says the impetus for the initiative stems from the rapidly growing scope of the ransomware threat.

It s no secret that ransomware, which encrypts data on users systems and then demands a ransom, has become a huge problem over the last few years, Naraine says. It has become so widespread that it could easily be called an epidemic, he says pointing to the sharp increase in the number of ransomware victims over the past year, from 131,000 in 2014-2015 to

718,000 over the past year.

Police and security researchers alone cannot fight the threat, Naraine says. Disrupting ransomware campaigns involves a coordinated effort between multiple stakeholders. Responsibility for the fight against ransomware is shared between the police, the justice department, Europol and IT security companies, he says.

Nomoreransom.org currently offers tools for decrypting data encrypted by the CoinVault, Rannoh, Rakhni and Shade crypto ransomware families. Victims of these malware samples and others like Autoit, Pletor, Rotor, Lamer and Lortok can use the tools to try and get their locked data back without having to pay any ransom for it.

The decryptor for Shade is the newest of the lot and was developed in June 2016 after a command and control server containing decryption keys for the ransomware was seized by law enforcement. The tool is designed to help users roll back the strong 256-bit AES encryption used by Shade to lockup user files.

The decryption tools currently available on nomoreransom.org are just the beginning, Kaspersky Lab and the other founders of the initiative said in a joint statement. Over the next few months expect the initiative to be expanded with participation from many more organizations and law enforcement agencies around the world.

This collaboration goes beyond intelligence sharing, consumer education, and takedowns to actually help repair the damage inflicted upon victims, said Raj Samani, chief technology officer of Intel Security s Europe, Middle East and Asia regions. By restoring access to their systems, we empower users by showing them they can take action and avoid rewarding criminals with a ransom payment.

The nomoreransom.org initiative is another indication of the level of concern caused by the spread of ransomware over the past year. In addition to individual Internet users, many of the cyber extortion attacks have targeted organizations as well, including those in the healthcare and government sectors.

The crypto protocols used to encrypt data in many of these attacks have been so strong and sophisticated that victims have had little option but to pay the demanded ransom to get their data back.

Security researchers and law enforcement authorities have warned against the trend and said that paying ransoms only encourages more attacks. But so far, few have offered victims any actual help in getting their encrypted data back.

Nomoreransom.org is the first initiative to attempt to do that and could well prove a turning point in the fight against the ransomware epidemic.

KeySniffer Lets Hackers Steal Keystrokes from Wireless Keyboards

Radio-based wireless keyboards and mice that use a special USB dongle to communicate with your PC can expose all your secrets your passwords, credit card numbers and everything you type.

Back in February, researchers from the Internet of things security firm Bastille Networks demonstrated how they could take control of wireless keyboards and mice from several top vendors using so-called MouseJack attacks.

The latest findings by the same security firm are even worse.

Researchers have discovered a new hacking technique that can allow hackers to take over your wireless keyboard and secretly record every key you press on it.

Dubbed KeySniffer, the hack is death for millions of wireless, radio-based keyboards.

The KeySniffer vulnerability affects wireless keyboards from eight different hardware manufacturers that use cheap transceiver chips (non-Bluetooth chips) a less secure, radio-based communication protocol.

The issue with these chips is that they don t receive Bluetooth s frequent security updates.

Moreover, the affected keyboards use unencrypted radio transmission.

This means anyone within 100 meters range of your computer and around $15-$30 long-range radio dongle can intercept the communications between affected wireless keyboards and your computer.

Eventually, this allows the attacker to collect secretly everything you type, including your passwords, credit card numbers, personal messages and even weird porn searches.

The keyboards from a surprising range of vendors, including Anker, EagleTec, General Electric, Hewlett-Packard, Insignia, Kensington, Radio Shack, and Toshiba, are vulnerable to KeySniffer.

This isn t the first time researchers have targeted wireless keyboards. In 2015, a white hat hacker developed a cheap Arduino-based device, dubbed KeySweeper, which covertly logs, decrypts and reports back all keystrokes from Microsoft wireless keyboards.

Although KeySweeper was due to the weak encryption used by Microsoft, the KeySniffer discovery is different as in this case; manufacturers are actually making and selling wireless keyboards with no encryption at all. One of the affected hardware makers, Kensington responded to this matter, saying that only a single version of its keyboards was affected by KeySniffer flaw and that a firmware update with AES encryption has been released.

Since there are millions of people who do use one of the wireless keyboards identified by Bastille Networks, it has been advised to you to either go back to the wires or at least switch to Bluetooth.

The radio-based wireless keyboards and mice are a good target for hackers. Two months back, the FBI also issued warning for private industry partners to look out for highly stealthy keyloggers that quietly sniff passwords and other input data from wireless keyboards.

Hacker Downloaded Vine’s Entire Source Code. Here s How...

Guess What? Someone just downloaded Twitter s Vine complete source code.

Vine is a short-form video sharing service where people can share 6-second-long looping video clips. Twitter acquired the service in October 2012.

Indian Bug bounty hunter Avinash discovered a loophole in Vine that allowed him to download a Docker image containing complete source code of Vine without any hassle.

Launched in June 2014, Docker is a new open-source container technology that makes it possible to get more apps running on the same old servers and also very easy to package and ship programs. Nowadays, companies are adopting Docker at a remarkable rate.

However, the Docker images used by the Vine, which was supposed to be private, but actually was available publically online.

While searching for the vulnerabilities in Vine, Avinash used Censys.io an all new Hacker s Search Engine similar to Shodan that daily scans the whole Internet for all the vulnerable devices.

Using Censys, Avinash found over 80 docker images, but he specifically downloaded ’vinewww’, due to the fact that the naming convention of this image resembles www folder, which is generally used for the website on a web server.

After the download was complete, he ran the docker image vinewww, and Bingo!

The bug hunter was able to see the entire source code of Vine, its API keys as well as third-party keys and secrets. "Even running the image without any parameter, was letting me host a replica of VINE locally," he wrote.

The 23-year-old reported this blunder and demonstrated full exploitation to Twitter on 31 March and the company rewarded him with $10,080 Bounty award and fixed the issue within 5 minutes.

Avinash has been an active bug bounty hunter since 2015 and until now has reported 19 vulnerabilities to Twitter.

PornHub Pays Hackers $20,000 To Find Zero-day Flaws in Its Website

Cyber attacks get bigger, smarter, more damaging.

P*rnHub launched its bug bounty program two months ago to encourage hackers and bug bounty hunters to find and responsibly report flaws in its services and get rewarded.

Now, it turns out that the world’s most popular p*rn*graphy site has paid its first bounty payout. But how much?

US $20,000!

Yes, P*rnHub has paid $20,000 bug bounty to a team of three researchers, who gained Remote Code Execution (RCE) capability on its servers using a zero-day vulnerability in PHP the programming language that powers P*rnHub's website.

The team of three researchers, Dario Weißer (@haxonaut), cutz and Ruslan Habalov (@evonide), discovered two use-after-free vulnerabilities (CVE-2016-5771/CVE-2016-5773) in PHP's garbage collection algorithm when it interacts with other PHP objects.

One of those is PHP's unserialize function on the website that handles data uploaded by users, like hot pictures, on multiple paths, including:

    http://www.P*rnH*b.com/album_upload/create
    http://www.P*rnH*b.com/uploading/photo

This zero-day flaw let the researchers reveal the address of the server's POST data, allowing them to craft a malicious payload and thereby executing rogue code on P*rnHub's server.

The hack was complicated and required a massive amount of work that granted a "nice view of P*rnHub s /etc/passwd file," allowing the team to execute commands and make PHP run malicious syscalls.

The PHP zero-day vulnerabilities affect all PHP versions of 5.3 and higher, though the PHP project has fixed the issue.

The hack could have allowed the team to drop all P*rnHub data including user information, track its users and observe behavior, disclose all source code of co-hosted websites, pivot deeper into the network and gain root privileges.

P*rnHub paid the team $20,000 for their incredible efforts, and the Internet Bug Bounty HackerOne also awarded the researchers an additional $2,000 for discovering the PHP zero-days.

The sophisticated hack on P*rnHub's servers that allowed the team to gain full access to the entire P*rnHub database has been explained in two highly detailed blog posts. You can head on to them for technicalities of this attack.

Using VPN in the UAE? You'll Be Fined Up To $545,000 If Get Caught!

If you get caught using a VPN (Virtual Private Network) in Abu Dhabi, Dubai and the broader of United Arab Emirates (UAE), you could face temporary imprisonment and fines of up to $545,000 (~Dhs2 Million).

Yes, you heard that right.

Online Privacy is one of the biggest challenges in today's interconnected world. The governments across the world have been found to be using the Internet to track people s information and conduct mass surveillance.

Here VPNs and proxy servers come into Play.

VPNs and proxy servers are being used by many digital activists and

protesters, who are living under the most oppressive regimes, to protect their online activity from prying eyes.

However, using VPN or proxy in the UAE could land you into great difficulty.

The UAE President Sheikh Khalifa bin Zayed Al Nahyan has issued new sovereign laws for combating cyber crimes, which includes a regulation that prohibits anyone, even travelers, in the UAE from using VPNs to secure their web traffic from prying eyes.

According to the laws, anyone using a VPN or proxy server can be imprisoned and fined between $136,000 and $545,000 (Dhs500,000 and Dhs2 Million).

The laws have already been issued by the UAE President and have now been reported to the official government news service WAM.

For those unfamiliar, Virtual Private Network (VPN) securely routes your Internet traffic through a distant connection, protecting your browsing, hiding your location data and accessing restricted resources.

Nowadays, VPNs have become a valuable tool not just for large companies, but also for individuals to dodge content restrictions as well as to counter growing threat of cyber attacks.

The UAE's top two telecom companies, Etislat and Du, have banned VoIP - the phone calling features in popular apps like WhatsApp, Viber, Facebook Messenger and SnapChat that deliver voice calls over the Internet for free - from within the Gulf nation.

However, soon the vast number of UAE residents who use VPNs and proxies within the UAE for years to bypass the VoIP ban could be in difficulty.

Out of two new laws issued last week, one lays out fines for anyone who uses a VPN or proxy server, local news reports. The new law regarding VPNs states:

"Whoever uses a fraudulent computer network protocol address (IP address) by using a false address or a third-party address by any other means for the purpose of committing a crime or preventing its discovery, shall be punished by temporary imprisonment and a fine of no less than Dhs500,000 and not exceeding Dhs2 million, or either of these two penalties."

The new move is in favor of telecom companies for whom VoIP 'over-the-top' apps have long been a major issue, as consumers no longer need to pay international calling rates to speak to their loved ones.

Warning: Over 100 Tor Nodes Found Designed to Spy On Deep Web Users

Researchers have discovered over 100 malicious nodes on the Tor anonymity network that are "misbehaving" and potentially spying on Dark Web sites that use Tor to mask the identities of their operators.

Two researchers, Amirali Sanatinia and Guevara Noubir, from Northwestern University, carried out an experiment on the Tor Network for 72 days and

discovered at least 110 malicious Tor Hidden Services Directories (HSDirs) on the network.

The nodes, also known as the Tor hidden services directories (HSDirs) are servers that act as introductory points and are configured to receive traffic and direct users to hidden services (".onion" addresses).

In other words, the hidden services directory or HSDir is a crucial element needed to mask the true IP address of users on the Tor Network. But, here s the issue:

HSDir can be set up by anyone.

"Tor’s security and anonymity is based on the assumption that the large majority of its relays are honest and do not misbehave," Noubir says. "Particularly the privacy of the hidden services is dependent on the honest operation of hidden services directories (HSDirs)."

The pair introduced around 1,500 honeypot servers, which they called HOnions (Honey Onions), running a framework to expose "when a Tor relay with HSDir capability has been modified to snoop into the hidden services that it currently hosts."

After the experiment, conducted between February 12, 2016, and April 24, 2016, the researchers gathered and analyzed all the data, revealing they identified at least 110 malicious HSDirs, most located in the US, Germany, France, UK and the Netherlands.

Over 70 percent of these 110 malicious HSDirs were hosted on professional cloud infrastructures, making it hard to learn who is behind the malicious nodes.

Furthermore, 25 percent of all 110 malicious HSDirs functioned as both HSDir and Exit nodes for Tor traffic, allowing the malicious relays to view all unencrypted traffic, conduct man-in-the-middle (MitM) attacks, and snoop on Tor traffic.

The paper, "Honions: Towards Detection and Identification of Misbehaving Tor HSDirs," [PDF] describes the researchers work in detail and will be presented next week at the DEF CON security conference.

While most malicious nodes queried for data like server root paths, description.json server files, and the Apache server status updates, others carried out malicious attacks such as XSS, SQL injection attacks, and path traversal attacks.

"We detected other attack vectors, such as SQL injection,..., username enumeration in Drupal, cross-site scripting (XSS), path traversal (looking for boot.ini and /etc/passwd), targeting Ruby on Rails framework (rails/info/properties), and PHP Easter Eggs (?=PHP*-*-*-*-*)," the research paper reads.

The researchers presented their findings on Friday at the Privacy Enhancing Technologies Symposium in Germany.

The researchers say Tor Project is aware of the HSDir issue and is working to identify and remove malicious HSDirs from the network.

"As far as we can tell, the misbehaving relays’ goal in this case is just to discover onion addresses that they wouldn’t be able to learn other

ways they aren’t able to identify the IP addresses of hosts or visitors to Tor hidden services," the Tor Project says in its blog.

Although Tor Project is working to remove malicious HSDirs, the long-term solution is a new design for hidden services: Mission: Montreal!

The code of the new design has been written, but a release date is still to be finalized, as the project says, "Tor developers finished implementing the protocol several months ago, and since then we’ve been reviewing, auditing, and testing the code."

According to the Tor developers, the new design will deploy a distributed random generation system that has "never been deployed before on the Internet."

Attacks on Tor are nothing new for Tor Project. This research is the latest indication for hidden services and Tor users that the network can not ultimately guarantee their anonymity.

Last year, the FBI unmasked TOR users in an investigation of the world s largest dark web child pornography website ’Playpen’ using its "Network Investigative Technique" (NIT) that remains undisclosed to this day.

The Tor Project reportedly accused the FBI of paying the security researchers of Carnegie Mellon University (CMU) at least $1 Million to disclose the technique they had discovered that could help them unmask Tor users.

The researchers canceled their talk demonstrating a low-cost way to de-anonymize Tor users at 2014 s Black Hat hacking conference with no explanation. The project has since patched the issues that made the FBI’s exploit possible.

Recently, the MIT researchers have created Riffle a new anonymity network that promises to provide better security against situations when hackers introduce rogue servers on the network, a technique to which TOR is vulnerable, though it is a long way from becoming reality.

End of SMS-based 2-Factor Authentication; Yes, It’s Insecure!

SMS-based Two-Factor Authentication (2FA) has been declared insecure and soon it might be a thing of the past.

Two-Factor Authentication or 2FA adds an extra step of entering a random passcode sent to you via an SMS or call when you log in to your account as an added layer of protection.

For example, if you have 2FA enabled on Gmail, the platform will send a six-digit passcode to your mobile phone every time you sign in to your account.

But, the US National Institute of Standards and Technology (NIST) has released a new draft of its Digital Authentication Guideline that says SMS-based two-factor authentication should be banned in future due to security concerns.

Here’s what the relevant paragraph of the latest DAG draft reads:

"If the out of band verification is to be made using an SMS message on a public mobile telephone network, the verifier SHALL verify that the pre-registered telephone number being used is actually associated with a mobile network and not with a VoIP (or other software-based) service. It then sends the SMS message to the pre-registered telephone number. Changing the pre-registered telephone number SHALL NOT be possible without two-factor authentication at the time of the change. OOB [Out of band verification] using SMS is deprecated, and will no longer be allowed in future releases of this guidance."

Due to rise in data breaches, two-factor authentication has become a standard practice these days. Many services are offering SMS-based 2FA to its consumers, just to ensure that hackers would need both their passwords and mobile phone in order to hack their accounts.

However, NIST argues that SMS-based two-factor authentication is an insecure process because it’s too easy for anyone to obtain a phone and the website operator has no way to verify whether the person who receives the 2FA code is even the correct recipient.

In fact, SMS-based two-factor authentication is also vulnerable to hijacking, if the individual uses a voice-over-internet protocol (VoIP) service, which provides phone call service via a broadband internet connection instead of a traditional network.

Since some VoIP services allow the hijacking of SMS messages, hackers could still gain access to your accounts protected with SMS-based two-factor authentication.

Also, the designing flaws in SS7 or Signalling System Number 7 also allows an attacker to divert the SMS containing a one-time passcode (OTP) to their own device, which lets the attacker hijack any service, including Twitter, Facebook or Gmail, that uses SMS to send the secret code to reset account password.

Even some devices leak secret 2FA code received via SMS on the lock screen.

The DAG draft notes that two-factor authentication via a secure app or biometrics, like a fingerprint scanner, may still be used to secure your accounts.

"Therefore, the use of biometrics for authentication is supported, with the following requirements and guidelines: Biometrics SHALL be used with another authentication factor (something you know or something you have)," the draft reads.

Moreover, Many tech companies such as Facebook and Google offer in-app code generator as an alternative solution for two-factor authentication, which does not rely on SMS or Network carrier.

Last month, Google made its two-factor authentication a lot easier and faster by introducing a new method called Google Prompt that uses a simple push notification where you just have to tap on your mobile phone to approve login requests.

Why Instagram’s Plans To Combat Online Harassment Won’t Work on Twitter

Since the beginning of the internet, online harassment has been a problem. We created this big, beautiful digital landscape that lets people be completely unfiltered, and we all do different things with this freedom. I, for example, use my platform to make sex memes and lightly neg Silicon Valley billionaires. Others take this opportunity to become the most scary-ass, shitbag, bigoted versions of themselves, hiding behind the comfy anonymity of their computer screens, facing no real consequences for threatening to rape, kill, and torture people.

Since it looks not great for social media companies to allow this on their platforms not addressing bad behavior condones it, according to the liberal lamestream media companies are now scrambling to deal with their massive abuse problems.

So on Friday, Instagram announced its plan to let users filter their comment streams, which came as no surprise. The Facebook-owned, image-sharing network plans to let each user build their own banned words list to filter out comments on their posts, a smart move that is mindful of the reality that everybody s definition of harassment is different. The Washington Post reported that users will also have the ability to turn off comments for individual posts, while The Verge claims that Instagram has yet to decide whether it will let all users disable comments.

This comes on the heels of some recent high profile harassment incidents on Twitter, the nerdy debate team president to Instagram s hot popular girl. In the past weeks and months and years the microblogging network has taken a lot of flack for the way it deals with abuse. Actress Leslie Jones quit the network after being the victim of a horribly racist campaign, initiated, in part, by Breitbart tech blogger Milo Yiannopolous. After receiving a flood of bad press about all this, Twitter fired back by banning Yiannopolous from its site.

Milo Yiannopoulos, the Breitbart blogger better known as @Nero on Twitter, has been permanently

The Verge wrote that Instagram is building the anti-harassment tools Twitter won t. While Instagram s new plan is clever the easiest way to make your users happy is to give them the choice to use it however the fu*k they want, which is what the new plan appears to do there is a reason Twitter has a more difficult time dealing with these issues.

Instagram is a photo-sharing network. Its purpose is to allow users to brag about their brunches with bae (f***ing murder me), cute dogs, fire memes, and selfies with friends. Comments are a secondary feature on the platform, so allowing each person to be in complete control of how people respond to their posts makes sense. At its core, Instagram is pictures. Without a comments section, the network would still flourish.

Instituting the same strict comment moderation policies on Twitter isn t a possibility because Twitter is the comments section. Twitter in its very structure creates a flawed kind of level playing field, writes Davey Alba at Wired. The network assigns the same inherent value to a tweet and a reply. Turning off or filtering out words you don t like for your replies would defeat the purpose of Twitter: screaming your hot takes and dumb jokes into a chaotic void. Some voices are inevitably louder than others, because of a sexy blue checkmark or lots of followers.

I ve heard people argue Twitter needs abuse to survive, in part because

it s desperate for more monthly active users it has a paltry 310 million, compared to Instagram s 500 million. But really, it s about what ultimate purpose these networks serve and why people decide to use them. People log on to Twitter to express their worldview, to make jokes and vent with other users about both the personal and the political. Instagram is for posting pictures. That s why this will work for them.

There is no one size fits all method to fixing online abuse. While every major social network should be working hard to combat the harassment their platforms facilitate, at the end of the day, social media serves as an echo chamber for people s shitty and offensive takes. The internet is full of harassment because the world is full of harassment. Filtering out offensive phrases in the comments section is placing a little bit of gauze onto an open infected wound: it ll help the bleeding, but it won t cure sh*t.

Microsoft Is Updating Windows 10 Again, in Its Latest Bid To Win You Back

A new update to Microsoft’s Windows 10 is coming, but you’re forgiven if you didn’t know. It turns out not many people are going to tell you.

Admittedly, there’s not much to talk about. The list of refinements for Microsoft’s free paper-anniversary update to Win 10 can fit on a small sheet with less than a dozen bullet points. The changes boil down to features like making the digital pen more useful, new technology to detect hacking attacks and the ability to log into a computer with a wearable device instead of a password.

The company’s Cortana voice-activated assistant will gain new features too, each of which was designed to bring the technology closer to, as Microsoft spokeswoman Laura Jones put it, "the same features of a real-life personal assistant."

With this in mind, Microsoft and the PC industry are largely treating the August 2 launch as just another Tuesday.

That’s just fine to Roger Kay, an analyst at Endpoint Technologies Associates, who said Microsoft is better off focusing its efforts on convincing businesses to upgrade than teaching consumers - who largely don’t know what version of Windows they’re running anyway - about an incremental upgrade. "People are probably not very excited by it," he said.

This is not the Microsoft you might remember from days of old, when the company and its partners would plow considerable resources into informing the world that a new version of Windows has arrived. In the years since Windows 8’s debut in 2012, when the company spent hundreds of millions of dollars spent telling the world about it, Microsoft has signaled change.

Satya Nadella took the reins as Microsoft’s new CEO two years ago, the Windows leadership team has changed, and the company is now releasing its widely used Word, Excel and PowerPoint Office software for phones and tablets, not just PCs. It’s even begun releasing new pet projects first, like a computer intelligence-powered camera app for Apple’s iPhone.

Windows is changing as well. The software behemoth is making good on its promise to run Windows "as a service," meaning it will send refinements and new features to PCs a couple of times a year. The result is our PCs

get new features quicker, and regular refinements of existing ones.

Microsoft also offered its latest Windows 10 software for free to nearly everyone who bought a PC in the past decade, a break with its tradition of charging hundreds of dollars for upgrades. That offer ended Friday.
Learning from the past

The PC makers say they're changing too. No longer focused on the computer-equivalent of talking about horsepower all the time, companies have settled on discussing the "experience" of using a computer. The new software, called "Windows 10 Anniversary Update," it just a part of the overall puzzle.

Dell has opted to market its computers in two ways: ads showcasing how good they look, and others about what people do with them (like making the Ghostbusters reboot). After all, why spend time marketing Windows features every other computer maker offers? "HP has Cortana too," said Allison Dew, head of marketing for Dell's PCs.

HP has also chosen not to directly market Windows or its features. "Our job is testing the new PCs shipping with the anniversary release and testing existing PCs," said Mike Nash, VP of customer experience and portfolio strategy at HP.

To be sure, that's not a small job. In recent years, HP has stepped up its communication with Microsoft in an effort to make sure its computers offer the best experience running the latest Windows 10 features, not merely support them.

As part of that effort, Nash, who used to work at Microsoft before leaving for Amazon and eventually HP, identified the most frustrating problems with computers and sought to fix them one-by-one. Among the changes, PCs start up faster these days and battery life is getting better too.

Dell, for its part, is continuing its efforts to break with the perception that it makes bare-bones ugly workhorse PCs. "The perception of Dell as innovative is starting to turn around," Dew said.

It's unclear whether that's enough at a time when Microsoft and the PC industry are clawing back respect from customers wooed by tablets, impressed by Apple's Mac laptops, or frustrated by Windows 8.

"Is it going to stem the tide in terms of migration from the PC to mobile devices? Absolutely not," said Van Baker, an analyst at Gartner. Still, he said, Windows Anniversary Update is worth the download.

=~=~=~=